IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:	
WHITE CHEVROLET CAMARO, BEARING PENNSYLVANIA REGISTRATION KXP 4816, INCLUDING THE VEHICLE ELECTRICAL AND DASHBOARD SYSTEM AND ANY AND ALL ELECTRONIC DEVICES FOUND WITHIN	Magistrate No. 25-728
HEWLETT PACKARD LAPTOP SERIAL: 5CG4253WGB	Magistrate No. 25-729
BLACK SAMSUNG CELL PHONE IMEI: 350962375761712	Magistrate No. 25-730
RED APPLE IPHONE	Magistrate No. 25-731
GREY/SILVER APPLE IPHONE	Magistrate No. 25-732

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Armando Gonzalez Jr, being first duly sworn, hereby depose and state as follows:

1. I have been employed as a Postal Inspector with the United States Postal Inspection Service (USPIS) since January of 2024. My duties include the investigation of crimes that involve the United States Postal Service (USPS) and the U.S. mail. These crimes include mail fraud, mail theft, identity theft, burglaries and robberies of post offices, and counterfeit postal money orders. I am currently assigned to the External Crimes Team within the Pittsburgh Office.

2. In the course of my training and experience, I have become familiar with the methods and techniques associated with the investigations of white-collar schemes to defraud. During these investigations, I have been involved in preparing and executing search warrants that have led to seizures of evidence of federal crimes.

3. This affidavit is submitted in support of an application for a search warrant, to search a Chevrolet Camaro (TARGET VEHICLE), any electronic devices located within the vehicle, and the TARGET VEHICLE's electrical and dashboard systems.

4. The TARGET VEHICLE is in the secure possession of the USPIS located at 1001 California Ave Pittsburgh, PA 15290. The TARGET VEHICLE was recovered after the arrest of Steven Goldwire (GOLDWIRE) on April 14, 2025. Your Affiant submits that there is probable cause to believe that the TARGET VEHICLE, any electronic devices therein, and the vehicle's dashboard system will contain evidence of violations of 18 U.S.C. §§ 1708, 1344, and 1349.

5. This affidavit is also submitted in support of an application for search warrants for three cellular telephones and a laptop further identified as the TARGET DEVICES. The TARGET DEVICES can further be described as:

a. Hewlett Packard laptop with serial number 5CG4253WGB (TARGET DEVICE #1);

b. Black Samsung Cell Phone with IMEI 350962375761712 (TARGET DEVICE #2);

c. Red Apple iPhone (TARGET DEVICE #3); and

d. Grey / Silver Apple iPhone (TARGET DEVICE #4).

6. The TARGET VEHICLE and TARGET DEVICES are further described in Attachments A-1 through A-5. This warrant seeks permission to search the places identified in Attachments A-1 through A-5, for the items identified in Attachment B. Because this affidavit is meant only to establish probable cause for the sought after warrant, it does not include every fact known to me as part of this investigation.

PROBABLE CAUSE

7. Over the last year the U.S. Postal Inspection Service (USPIS) has seen an increase in mail stolen from the United States Postal Service (USPS) blue collection boxes. The theft of mail and checks from the collection boxes has led to the negotiation of counterfeit checks as well as bank customer impersonation frauds in Western Pennsylvania and throughout the United States. Mail theft is a violation of 18 U.S.C. § 1708. Bank fraud and conspiracy to commit bank fraud are violations of 18 U.S.C. §§ 1344 and 1349.

8. As a result of this activity, USPIS inspectors in Pittsburgh have utilized cameras, motion detection devices, and trackers in the USPS blue collection boxes located in areas known to experience high volumes of mail theft. These areas include Pittsburgh, PA, Penn Hills, PA, Millvale, PA, Mt. Lebanon, PA, and West Mifflin, PA.

9. On April 10, 2025, at approximately 2:28am, a covert camera installed by USPIS at the Penn Hills Post Office captured an incident of mail theft. The camera captured a white Chevrolet Camaro (TARGET VEHICLE) operated by a male subject later identified as Steven Goldwire (GOLDWIRE). GOLDWIRE is observed parking the vehicle directly next to the blue collection box, removing all the mail, and dumping it in the TARGET VEHICLE.

10. The TARGET VEHICLE is a newer model, white body, with a black soft top/roof, and a black stripe/marking on the hood.

11. On the evening of April 13, 2025, Your Affiant placed a packaged GPS tracking device in the blue collection box at the Penn Hills Post Offices for the purposes of tracking the mail. During the evening of April 13, 2025, and early morning of April 14, 2025, USPIS inspectors conducted physical surveillance at the Penn Hills Post Office.

12. On April 14, 2025, at approximately 2:29 AM, the TARGET VEHICLE is observed by USPIS inspectors arrive at the Penn Hills Post Office and park immediately next to the blue collection boxes. Inspectors observed the individual later identified as GOLDWIRE exit the TARGET VEHICLE, approach the blue collection box, remove the mail contained within, and place it into the TARGET VEHICLE.

13. The individual later identified as GOLDWIRE is observed as a black male, slim build, and wearing a dark and white colored hooded jacket. He is also observed wearing a blue surgical mask.

14. Postal Inspectors approached the TARGET VEHICLE with lights and sirens initiated, in an attempt to stop GOLDWIRE. Upon seeing inspectors, GOLDWIRE reentered the TARGET VEHICLE and fled the scene at a high rate of speed.

15. Utilizing the GPS tracking device placed in the mail, Postal Inspectors verified that the GPS tacking device was stolen and located at the Comfort Inn at 699 Rodi Rd Pittsburgh, PA 15235. The Comfort Inn is located approximately 1.9 miles from the Penn Hills Post Office.

16. Upon arrival at the Comfort Inn, Inspectors located the TARGET VEHICLE in the Comfort Inn parking lot. The located TARGET VEHICLE had the same aforementioned characteristics as the Chevrolet Camaro which had engaged in mail theft at the Penn Hills Post Office. Inspectors and Officers observed the Vehicle Identification Number (VIN) on the TARGET VEHICLE to be scratched off, indicative it was stolen. The TARGET VEHICLE had a Pennsylvania license plate KXP 4816 attached to it. Inspectors determined the license plate did not correspond to the TARGET VEHICLE.

17. Postal Inspectors reviewed video surveillance at the Comfort Inn and located video of the TARGET VEHICLE arriving at The Comfort Inn at approximately 2:32am.[1] The video further shows GOLDWIRE enter the front lobby wearing the same clothing worn by the mail theft suspect.

18. GOLDWIRE is captured on surveillance cameras walk through the lobby and enter the 2A hallway. As GOLDWIRE entered the 2A hallway, he began removing his jacket and placed the jacket in front of door 209. GOLDWIRE is observed on surveillance video dropping a surgical mask on the ground while walking through the 2A hallway. After removing his jacket, GOLDWIRE is seen in the hallway wearing a white tank top style undershirt. GOLDWIRE is then seen leaving hallway 2A. While leaving hallway 2A, GOLDWIRE'S face is clearly captured on camera.

19. The Comfort Inn advised that the rooms on the second floor, which includes room 209, have access to the outside through an exterior sliding door located in the room.

20. At approximately 2:42am, surveillance video from the exterior of the "A" wing of the Comfort Inn, and in the immediate area of 209, showed GOLDWIRE wearing all black clothing walking in the parking lot. Approximately one minute later, the TARGET VEHICLE is seen on video being parked on the "B" side of the Comfort Inn parking lot. GOLDWIRE exited the TARGET VEHICLE possessing a dark duffle bag. GOLDWIRE is observed on surveillance cameras walking past the lobby doors and towards the area of room A209.

21. At approximately 2:50am, surveillance video from the Comfort Inn captured GOLDWIRE stick his head out from room 209. Seconds later, GOLDWIRE exits room 209

[1] This is the time reflected by the security system at the Comfort Inn, which may not be perfectly precise. All of the times that follow in this affidavit are based on the Comfort Inn security system.

carrying the black duffle bag and walks to the ice machine vending area on hallway 2A. The ice machine vending area is located three (3) doors from room 209. GOLDWIRE enters the ice machine vending area and walks out seconds later without the duffle bag.

22. After reviewing the video, Your Affiant went to the ice machine and vending area located in the 2A hallway and discovered the dark duffle bag hidden in the room. Your Affiant observed the duffle bag laying on the ground, opened, and with numerous visible pieces of mail. A preliminary review of the duffle bag revealed it contained approximately 321 pieces of presumed stolen mail. The GPS tracker which was placed by Your Affiant in the blue bin collection box at the Penn Hills Post Office on April 13, 2025, was in the duffle bag. Inspectors later discovered the trash bin in the ice machine and vending area contained a bag filled with stolen mail.

23. While inside the hotel, Postal Inspector Staci McCoullough observed GOLDWIRE exit room 209. Postal Inspectors in the hotel lobby area observed GOLDWIRE walkthrough the lobby wearing a white tank top style undershirt and dark pants. Your Affiant identified GOLDWIRE as the individual seen on video surveillance enter the Comfort Inn wearing the clothing similar to that worn by the individual that committed the mail theft at Penn Hills.

24. Postal Inspectors approached GOLDWIRE, in an attempt to identify him. GOLDWIRE identified himself but was untruthful about the room he was staying in. Postal Inspectors detained GOLDWIRE and determined he was in possession of a red Apple iPhone (TARGET DEVICE #3) with a black case, a grey/silver Apple iPhone (TARGET DEVICE #4) with a clear black case, and two (2) Western Union money orders made out to "Pittsburgh Water" and "Department of Transportation, presumed to be stolen. GOLDWIRE was also in possession of a surgical mask, which appeared similar to that worn by the suspect during the mail theft in Penn Hills.

25. Comfort Inn records revealed Steven Ihsan of 1624 East Howell Street Philadelphia, PA 19149, with a telephone number: 445-220-1756, was a guest staying in room 209. Further records reveal GOLDWIRE checked in at the hotel on April 10, 2025, with a reservation for four (4) nights.

26. While canvasing the hotel area, Inspectors located a key fob belonging to a Chevrolet, laying on the ground between the lobby and hallway "2A". Inspectors confirmed the key fob belonged to the TARGET VEHICLE. Inspectors also located a temporary vehicle registration tag in the trash bin near the "A" side exterior entrance.

27. At approximately 12:30 PM, Inspector Anderchak, Inspector McCullough, Inspector Bohin and Task Force Officer DeGori, executed a federal search warrant on room #209 at the Comfort Inn. The search uncovered additional evidence of mail theft, bank fraud and conspiracy to commit bank fraud. Inspectors located approximately 200 stolen checks in USPS Express envelopes, a Hewlett Packard laptop (TARGET DEVICE #1), a black Samsung cell phone (TARGET DEVICE #2) and other evidence supporting the alleged crimes.

28. Your Affiant knows that electronic devices, including computers, laptops, printers, and cellular phones, can be used in furtherance of mail theft, bank fraud, and conspiracy. Specifically, these items can be used to communicate with co-conspirators, store banking information, store personally identifying information, and create counterfeit checks.

29. Based on my training and experience, I am aware that cellular telephones are often used in financial crimes to communicate with co-conspirators and others regarding the commission of the crimes, and that they are capable of storing information related to recent telephone calls, telephone directories, text messaging and other relevant information, such as location data.

30. Your affiant believes that the information contained within the TARGET DEVICES may reveal the identity of other conspirators, instructions to others regarding the crimes, as well as other communications made in furtherance of the conspiracy.

31. Without turning on and searching the phone, it is not possible to tell what telephone number is associated with the phones. With the authorization sought in this search warrant, your affiant will be able to identify the associated telephone number. A subpoena to the cellphone provider for this telephone number can then be completed to obtain additional details about the account holder, including associated addresses, telephone numbers and methods of payment.

32. Your Affiant also knows that the phones are capable of not only voice communications, but also text messaging, SMS chat messaging, and email communications. Your affiant also knows that the phones may also have significant electronic storage capability, as well as internet browsing and computer functions, and memory storage which may reveal additional evidence of the crimes.

33. Your Affiant also knows through training and experience that the perpetrators of financial crimes and identity theft crimes communicate by electronic means. And, that electronic devices such as computers, tablets, cell phones or other electronic storage devices are used to store bank routing and account numbers; debit/credit card account information; check templates; counterfeit checks; and the software to produce counterfeit checks and identification documents

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

34. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

35. There is probable cause to believe that things that were once stored on the TARGET DEVICES may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because

special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

36. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the TARGET DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

37. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

38. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

NATURE OF EXAMINATION

39. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of all the TARGET DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

MANNER OF EXECUTION

40. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

41. Based on the information above, your Affiant submits that there is probable cause to believe that evidence, instrumentalities, and proceeds of mail theft, in violation of 18 U.S.C. § 1708, bank fraud, in violation of 18 U.S.C. § 1344, and conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349, are located in the TARGET VEHICLE , TARGET DEVICE #1 and TARGET DEVICE #2, TARGET DEVICE #3, and TARGET DEVICE #4. Thus, your Affiant requests a warrant to search those items for the items described in Attachment B.

The above information is true and correct to the best of my knowledge, information and belief.

Respectfully submitted,

/s/ Armando Gonzalez Jr.
Armando Gonzalez Jr.
U.S. Postal Inspector,
U.S. Postal Inspection Service

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 24th day of April 2025.

_____
HONORABLE KEZIA O. L. TAYLOR
United States Magistrate Judge

Attachment A-1

Item to be Searched

The item to be searched is:

The TARGET VEHICLE, further described as a Chevrolet Camaro bearing the Pennsylvania License Plate KXP-4816. The TARGET VEHICLE is white in color, black soft top/room, with a black stripe/marking on the hood, along with any electronic devices located within the vehicle, and the TARGET VEHICLE's electrical and dashboard systems.

Attachment A-2

Item to be Searched

The item to be searched is:

TARGET DEVICE #1: Hewlett Packard laptop, pink in color, serial number: 5CG4253WGB.

Attachment A-3

Item to be Searched

The item to be searched is:

TARGET DEVICE #2: A black Samsung cell phone with the IMEI number: 350962375761712.

Attachment A-4

Item to be Searched

The item to be searched is:

TARGET DEVICE #3: The Red Apple iPhone with a black case recovered from Steven GOLDWIRE's person. TARGET DEVICE #3 is currently in the possession of United States Secret Service.

Attachment A-5

Item to be Searched

The item to be searched is:

TARGET DEVICE #4: The Grey/Silver Apple iPhone with a black clear case recovered from Steven GOLDWIRE's person. TARGET DEVICE #4 is currently in the possession of United States Secret Service.

Attachment B

Items to be Seized

1. All evidence, instrumentalities, proceeds, records and information relating to violations of Title 18, Sections 1708, 1344, and 1349, including:

a. Any and all records and information relating to the possession, sale, transfer, use, production, or trafficking of means of identification, counterfeit checks, account numbers, and other access devices associated with any financial institutions;

b. Any and all records of communications with financial institutions and co-conspirators in furtherance of the crimes under investigation;

c. Mail, including business, treasury, and personal checks, in names other than STEVEN GOLDWIRE or any other occupant of the hotel room;

d. USPS arrow keys and/or counterfeit arrow keys;

e. USPS property;

f. Any and all records and information relating to mail and other financial documents not in the name of STEVEN GOLDWIRE;

g. Any and all records and information that provide evidence of control or ownership of the premises or a Chevrolet Camaro;

h. Any articles of clothing that are evidence of mail theft;

i. Any passwords, password files, test keys, encryption codes or other information necessary to access the storage devices or data; and,

j. Records relevant to establishing the location of GOLDWIRE in relation to the crimes under investigation.